Information
and Privacy
Commissioner/
Ontario

Privacy and Digital Rights Management (DRM): An Oxymoron?

Ann Cavoukian, Ph.D.
Commissioner
October 2002

The Information and Privacy Commissioner/Ontario gratefully acknowledges the work of Pasha Peroff, Policy and Technology Analyst; Mike Gurski, Senior Policy and Technology Advisor; and Colin Bhattacharjee, Project Analyst.

This publication is also available on the IPC Web site.

Information and Privacy Commissioner/Ontario

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: www.ipc.on.ca

103-02274/

Table of Contents

Introduction 1

The Advent of Digital Rights Management (DRM) 3

The Impact of DRM on Privacy 4

- Integrating privacy into DRM technologies 6
- Step #1: Define the privacy expectations of the public and identify legislated requirements 7
  - Privacy expectations of the public 7
  - Legislated requirements 7
- Step #2: Develop privacy policies and principles 9
- Step #3: Undertake an assessment of human and information resources with a focus on personally identifiable data (collection, processing, managing data flows) 10
- Step #4: Undertake a threat risk assessment by completing a Privacy Impact Assessment .. 10
- Step #5: Deploy methodology for privacy risk management at the systems level 10
- Step #6: Introduce at the source level, the rules and controls developed in step #5 11
- Step #7: Deploy and audit, through a model of continuous improvement — review expectations and requirements 11

Privacy Protection Tips for Consumers 12

Conclusion 13

Appendix A — CSA *Model Code for the Protection of Personal Information* 14

Endnotes 16

Introduction

In May 2001, country singer Charley Pride released a new compact disk (CD), *A Tribute to Jim Reeves*. Pride is a well-known, multi-award winning artist, but his new CD contained a technological surprise.

To combat music piracy, a new copy-prevention technology was embedded in the CD that prevents consumers from "burning" or duplicating it. Moreover, the tracks on the CD could not be played on the CD audio players found in many personal computers.

Consumers could listen to the CD on a standard CD audio player. However, if they attempted to play it on their personal computers, they were directed to a Web site of SunnComm, the company that produced the copy-prevention technology. At this Web site, they could use Microsoft's Windows Media Player to download and listen to free digital versions of tracks from the CD.

Not all consumers were enthralled with this new copy-prevention technology. In September 2001, a California woman sued the record company (Fahrenheit Entertainment), its affiliate (Music City Records) and SunnComm for "maintaining a complex inter-related constellation of practices that have been designed and implemented to defeat the rights of consumers and consumers' reasonable expectations and that include misleading advertising, defective notices, and invasions of privacy."[1]

The lawsuit, which raised a host of consumer rights issues, alleged that the technology violated the privacy rights of consumers by storing their personally identifiable information, tracking their listening habits, and disseminating their personally identifiable information to third parties. In addition, the suit claimed that the record company had never disclosed on the shrink-wrap of the CD that consumers could not listen to music on their computers anonymously.[2]

According to the lawsuit, when consumers inserted the Charley Pride CD into the CD-ROM drive of their personal computer, they were directed to SunnComm's Web site, where they were asked to provide SunnComm with personal identifying information, including their e-mail address and full name. It further alleged that the defendants used "cookie, web bug and Digital Rights Management Technology to track specific consumer musical habits and clickstream data, combine it with personal identifying information, and provide such data and information to parties outside of the knowledge and control of the specific consumer...."[3]

In February 2002, the plaintiff and defendants settled the suit. The defendants agreed not to require consumers to provide personally identifiable information, such as their e-mail address or Internet Provider (IP) address, as a condition for listening to the Charley Pride CD on their computer or downloading songs from the SunnComm Web site. They also agreed to purge all personal identifying information obtained from consumers to date from the music file downloading process, and to amend their privacy policies to advise consumers that all downloads of songs from the CD on the SunnComm Web site now would be anonymous.[4]

This legal battle represents an early skirmish in a new conflict over privacy rights that may be developing between owners of intellectual property and consumers. One flashpoint for these battles is digital rights management (DRM), a scheme that involves using various forms of technology to secure digital content and protect it from being used, copied or distributed without the permission of the copyright holder. The copy-protection technology embedded on the Charley Pride CD is an example of such technology.

Consumer products such as music, movies and books are becoming more widely available in digital format, both in physical form (e.g., on a CD or DVD) and over the Internet (e.g., downloading a movie or song from a Web site). However, as illustrated by the Charley Pride CD case, the use of DRM technologies to protect such digital content may have privacy implications, particularly if they are used in conjunction with Internet tracking tools, such as cookies and web bugs, to collect and store personal information from consumers in order to monitor their behaviour and buying preferences.

The spread of DRM technologies has not gone unchallenged. For example, Stanford University Professor Lawrence Lessig has argued that the most dramatic restrictions on innovation on the Internet have come at the hands of copyright holders, such as large music-production companies. The push to provide these copyright owners with control over their content has also given them the power to stifle innovations that could threaten their existing business models.[5]

In addition, the Electronic Privacy Information Centre (EPIC), the Electronic Frontier Foundation (EFF), and other privacy advocates have ignited an important public debate by identifying the serious threat that DRM technologies pose to the privacy, fair use and free expression rights of consumers.[6]

The purpose of this paper is to contribute to this debate by focusing exclusively on the privacy implications of DRM. First, we will examine DRM in greater detail and outline some of the factors that gave rise to such technologies. Second, the impact of DRM on the privacy rights of consumers will be discussed. Third, we will put forward some proposals for embedding privacy into DRM technologies, including seven essential steps that DRM technology developers should consider to ensure that they are respecting the privacy rights of consumers. Finally, we will put forward some straightforward privacy tips for consumers who are planning to purchase or have purchased digital products protected by DRM technologies.

The Advent of Digital Rights Management (DRM)

In the early days of the Internet, the slogan "information wants to be free" was the catch phrase of the day, and the Internet was viewed as a vehicle for expanding democratic space and the exchange of ideas and information. At the same time, businesses saw the Internet as a platform for e-commerce – the buying and selling of goods in cyberspace. In particular, many corporations that hold copyright over music, movies and books viewed the Internet as a potential vehicle for marketing and selling these products in digital format to consumers.

These same corporations, however, also perceived the Internet as posing a threat to their ability to control the distribution of digital content. The development of "peer-to-peer" music-sharing networks such as Napster, and new technologies such as MP3 players, have greatly alarmed corporate copyright owners, who believe that such innovations promote online piracy of their intellectual property.

Corporate copyright owners have responded to this perceived threat by promoting the development of DRM. In a broad sense, DRM includes not only the technologies that are used to secure digital content from unauthorized distribution or copying, but also the laws, contracts and licenses that impose restrictions on the use of such material. Although DRM technologies are commonly used to protect commercial content (e.g., music and movies), they can also be used to protect other digital content, such as corporate information (e.g., legal documents) and personal information (e.g., medical records).[7]

However, DRM technologies are most commonly used to protect "popular" digital content such as music and movies from being copied, altered, saved, printed or transmitted to third parties. According to EPIC, DRM technologies secure content in two ways. First, they use "containment," which involves encrypting digital content in a shell so that only authorized users can access it. Second, they use "marking," which is the practice of placing a watermark, flag or XrML tag on content to signal to a device that the media is copy protected.[8]

In the United States, the advent of DRM has been accompanied by legislative protections. In 1998, the U.S. Congress passed the *Digital Millennium Copyright Act* (DMCA),[9] which bans technology designed to circumvent copyright protection technologies, such as DRM.

Both corporate giants – such as Microsoft – and smaller players – such as SunnComm – have developed DRM solutions. For example, several major music labels and online movie companies use Microsoft's Media Rights Manager to deliver digital content securely. Media Rights Manager provides content owners with the ability to limit the number of times a music or movie file can be played; to determine whether a file can be burned onto a CD; and to control whether a file may be copied onto a portable player or other device.[10] Similarly, smaller companies such as SunnComm have developed DRM technologies aimed at preventing music CDs from being copied.

The Impact of DRM on Privacy

In North America, the legal concept of privacy was first explored in an 1890 article in the *Harvard Law Review* by Professors Samuel Warren and Louis Brandeis, who defined privacy as "the right to be let alone."[11] This definition of privacy has evolved over the last century to include at least two strands: the right of individuals to control their physical space (i.e., their body or home) and to control their personal information. The latter right is known as "informational privacy" or "informational self-determination."

Consequently, privacy includes the right of individuals to control the collection, use and disclosure of personal information about themselves. Personal information can be defined generally as identifiable information about an individual. In other words, it is information that serves to identify a person and could include his or her name, address, telephone number, date of birth, race and family status. It could also include an identifying number that the government has assigned to an individual in exchange for receiving benefits, a person's e-mail address, and a person's medical or financial history.

Some companies that use DRM technologies rely on the technology's capacity to collect personal information and transmit it back to the publisher of the content. They may also use the personal information and other "click-stream" information as a means to track customers' demographics and usage patterns and, as a result, learn how to market to particular market segments more precisely.

IT experts have reported on the privacy problems associated with DRM technologies.[12] Not all DRM applications function in the same way. Some monitor content and rights acquisition, some focus on downloading extensions for advertising purposes, while some monitor and profile content usage; some may even execute all functions at once. What is relevant is that in virtually all cases, DRM requires the collection of personal information (data collected from the user's operation of the DRM application and the content it provides access to) in order to work properly.

According to a thoughtful paper entitled, *Privacy Engineering for Digital Rights Management Systems*,[13] privacy concerns arise in a number of ways, including:

1. **ID linkage:** This DRM model requires the user to provide an ID number that links the user's personal information (name, address, transaction history, etc.) with the device or service a person intends to use. (For example, the device could be a computer or cellphone.) These devices or services connect to a rights server (a catalogue of user access/usage rights associated with particular devices or services), so that when someone decides to use a device or service, or updates or changes to another device or service, the rights server catalogues these uses or changes using the initially registered ID provided by the user. The paper stresses, "[s]uch tracking for the purpose of tying content to a set of devices obviously puts at risk some previously private information about the user."[14] It is not clear, in most reports on the subject, which DRM applications actually catalogue and mine such ID numbers but, regardless, the capability still exists due to the "ongoing, periodic contact between user and distributor."[15]

2. **User tracking via download or subscription service:** This DRM model supplements the aforementioned ID linkage model. The DRM application requires that the user reconfirm that he or she will not copy a product for resale or sharing. At present, this is the most popular model for this type of data collection. The model not only catalogues the user under a user-specific ID, but also catalogues the customer's usage history of a product that has been downloaded from a system that is subscribed to and streamed whenever requested. The paper states that, "[t]his is a qualitatively more serious threat than those previously described. Many people would be willing to risk others knowing that they downloaded a pornographic video; fewer would want others to know that they watched this video 1,000 times."[16]

A similar DRM model allows for the potential collection of usage data that may occur when a user subscribes to a package of services. The user does not actually download anything to his or her system but instead receives streamed elements of the package by request. If the streamed elements are viewed or listened to, such actions can be recorded, resulting in the collection of an individual's interests and usage patterns.

As a result of the above-noted ability to collect and track personally identifiable information, DRM applications may allow for the creation of substantial, unregulated personal profiles. This ability not only creates the threat of inappropriate, non-consensual access to and disclosure of a customer's information, but also potentially provides other companies and law enforcement with a source of information on citizens by way of a court order or possibly by simply purchasing the information.[17]

Privacy abuses do not necessarily come from the storage of such personal information but more from the threat that such a database may be subject to a security breach that reveals a user's personal information. Worse yet, some companies view personal information obtained from customers as a corporate asset that can be sold during bankruptcy proceedings.[18]

Moreover, DRM systems, especially in the case of subscription-service-based systems, often create communication links between the user's and server's systems, which may be vulnerable to attacks from hackers and saboteurs. In this respect, some DRM systems require an open channel to feed data back and forth from user to the distributor in the same way that any distributed computing application requires users to maintain such channels (i.e., Instant Messenger, SETI@Home). Some DRM systems may actually be designed to harm a user's system.[19]

In short, the privacy-invasive effects of DRM technologies are rarely addressed. Nor do DRM developers typically attempt to design privacy into their products. Currently, many DRM models focus on ensuring that the rights of the content providers and service distributors are protected, without sufficient regard for consumer privacy. We believe that DRM developers should examine how the current DRM models can be adjusted to provide greater privacy protection for consumers.

Integrating privacy into DRM technologies

There are a number of both simple and complex measures that can be undertaken by both DRM developers and companies selling DRM-protected products to ensure that their technologies do not violate the privacy rights of consumers. As a starting point, companies that use DRM technologies should consider whether collecting personal information from consumers is even necessary.

In the settlement reached in the Charley Pride CD case, the defendants agreed not to require consumers to provide "personally identifiable" information, as a condition for listening to the CD or downloading songs from the SunnComm Web site. We would encourage other companies selling DRM-protected products to consider eliminating the collection of unnecessary personal information. If any personal information is collected, it should only be obtained with the consent of the consumer. Consent in this context should be "informed consent" – the consumer must understand the nature and consequences of providing or withholding consent.

If a consumer consents to the collection of his or her personal information, companies that use DRM should recognize that copyright holders and consumers actually share a common interest – controlling the flow of the information. For example, Harvard University Law Professor Jonathan Zittrain has argued that there is a profound relationship between those who wish to protect intellectual property and those who wish to protect privacy. Their common desire is control over the distribution of information.[20] Similarly, Mark Stefik, a research fellow and manager at the Xerox Palo Alto Research Center, has argued that the same technology that guards the property rights of publishers could also be used to protect the personal information of consumers.[21] Stefik outlines the manner in which this could be accomplished in an intriguing article in *Scientific American* titled "Trusted Systems."

The thrust of many DRM technologies is to control information that is protected by copyright laws. Similarly, a key element of personal privacy is that individuals should have the right to control the collection, use and disclosure of their personal information. Consequently, the DRM methodology for strictly controlling the distribution of intellectual property in digital form offers an ideal model for protecting the personal information of consumers. In other words, DRM developers should implement a scheme that ensures that any personal information collected from consumers is protected as zealously as intellectual property.

The following section explores ways to create such a scheme. In 2002, the Information and Privacy Commissioner/Ontario released a paper called, the *7 Essential Steps for Designing Privacy into Technology*,[22] which provides a framework for undertaking a privacy analysis of any technology and its related components, ranging from legal issues to policy practices. The *7 Steps* can be applied to DRM technologies in the following way:

Step #1: Define the privacy expectations of the public and identify legislated requirements

Privacy expectations of the public

In a consumer context, the success of new technologies is invariably linked to public acceptance. Consumers will not accept a new form of technology if it is costly, difficult to use or violates their rights to fair use, freedom of expression and privacy.

According to a recent Harris Interactive survey, 83% of American consumers would stop doing business with a company entirely if they heard or read that the company misused customer information.[23] A Forrester Research survey of both Americans and Canadians found that almost 90% of online consumers want the right to control how their personal information is used after it is collected.[24]

These survey results should serve as a reminder to companies that the consumer should be treated as a "first-class participant."[25] The relationship between a company that uses DRM and the consumer should be based on trust, co-operation and understanding. This can be at least partly achieved by respecting the privacy rights of consumers.

Legislated requirements

From a legal standpoint, DRM technology is inherently cross-jurisdictional because it often operates within an online environment. Web sites that make digital products available for sale or downloading can be accessed from anywhere in the world with an Internet connection. As a result, the legal requirements for organizations providing goods and services that can purchased by consumers living in various jurisdictions are often unclear.

The reality is that many companies that provide DRM-protected products, particularly on the Internet, are based in the United States. Currently, there is no comprehensive national privacy legislation in the U.S. that applies to the private sector. Congress has enacted sector-based privacy laws that apply to the financial and health sectors. However, companies that use DRM technologies to protect digital music, movies or books sold online are not subject to comprehensive privacy legislation that would apply to the collection, use and disclosure of a customer's personal information. Rather, individuals who believe that the use of DRM technology violates their privacy rights would have to rely on consumer protection statutes or in very limited cases, state privacy laws.

However, companies that use DRM technologies should be aware that comprehensive privacy legislation exists in other jurisdictions around the world. In 1995, the European Union (EU) passed the *Data Protection Directive*,[26] which sets out privacy-protection rules for personal information held by both government and private-sector entities and aims to harmonize data-protection rules in the EU. The directive also establishes rules designed to ensure that data (i.e., personal information) is only transferred to countries outside the EU, where continued privacy protection is guaranteed.

The 15 member states of the EU were required to implement the directive into national law by October 25, 1998. Consequently, many European countries have comprehensive privacy legislation that could apply to personal information of consumers that is collected, used or disclosed by European-based companies selling digital products that use DRM technologies. In addition, companies that use DRM technologies to protect digital music, movies, or books that are sold online to European customers should note that an EU Data Protection Working Party has published a paper that examines how EU data protection laws would apply to personal information processed on the Internet by non-EU based Web sites (e.g., in the U.S.). In particular, the paper notes that:

> The directive would also apply to information collected through spywares, which are pieces of software secretly installed in the individual's computer, for instance at the occasion of the downloading of bigger software (e.g. a music player software), in order to send back personal information related to the data subject (e.g. the music titles the individual tends to listen to) ... As these technologies are by definition used without informing the user (the name spyware is clear in that respect) they are a form of invisible and not legitimate processing.[27]

In Canada, the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)[28] applies to federally regulated private-sector organizations that collect, use or disclose personal information, either in paper or electronic format, in the course of their commercial activities. Consequently, PIPEDA would not likely apply to U.S. companies that use DRM technology to protect digital music, movies or books sold online to Canadian customers. However, PIPEDA could apply in certain circumstances to personal information that is collected, used or disclosed by any federally-regulated Canadian company (e.g., cable or telecommunications companies) that use DRM technologies to protect digital music, movies or books sold on Canadian Web sites.

In the absence of privacy legislation, companies that provide DRM-protected products should consider adopting fair information practices. In 1980, the Organisation for Economic Co-operation and Development (OECD) adopted the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[29] These guidelines include eight Basic Principles of National Application, commonly known as "fair information practices," and form the basis for virtually all privacy legislation around the world.

In 1996, the Canadian Standards Association (CSA) released a *Model Code for the Protection of Personal Information*,[30] which is based on the OECD *Guidelines*. The CSA *Model Code* includes the following 10 privacy principles:

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure, and Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

A detailed description and definition of each of these principles is included in *Appendix A* of this paper.

Step #2: Develop privacy policies and principles

Companies that use DRM can create easily accessible privacy policies either by using an online privacy policy generator[31] or by contracting the services of a reputable third party. Privacy policies should be based on the privacy legislation that applies to personal information collected in a particular jurisdiction, or on fair information practices if no legislation exists. Such policies should be displayed in a prominent place on a company's Web site and should be written in plain language.

A privacy policy should explain to consumers:

- what personal information is being collected;
- why it is being collected;
- how it will be used;
- who will have access to it;
- how long you will retain it;
- how you will dispose of it;
- who in the organization to contact for more information about the policy.

The IPC has published a set of privacy policy best practices, which are available at www.ipc.on.ca/english/pubpres/if-you/web-priv.htm.

Step #3: Undertake an assessment of human and information resources with a focus on personally identifiable data (collection, processing, managing data flows)

Companies that sell DRM-protected products should assess how their human resources (i.e., managers, employees) handle the personal information of consumers. In addition, they should conduct an assessment of how their informational resources (i.e., computer hardware and software) are used to collect, store and transmit personal information.

The IPC has developed, with the assistance of PricewaterhouseCoopers and Guardent, the freely available *Privacy Diagnostic Tool* (PDT),[32] which can be used by organizations to gauge their data handling processes against fair information practices. Once the tool's privacy questionnaire has been completed, the PDT generates a report summarizing the strengths and weaknesses of the organization's data-handling processes and provides suggested remedial next steps. We would recommend that companies develop a specific action plan dealing with issues of employee accountability, privacy awareness and levels of training around DRM.

Step #4: Undertake a threat risk assessment by completing a Privacy Impact Assessment

A *Privacy Impact Assessment* (PIA) provides an in-depth assessment of relevant privacy legislation, privacy implications of systems design, and consumer privacy expectations. Once privacy goals are determined and initial privacy vulnerabilities detected, the PIA should offer ongoing guidance each time a data collection process is created or modified. The Ontario government's Management Board Secretariat has created a PIA.[33] Other PIAs include the British Columbia government's Corporate PIA[34] and the Government of Canada's Treasury Board Secretariat PIA.[35]

Step #5: Deploy methodology for privacy risk management at the systems level

This step is crucial to the deployment of privacy-protective DRM technologies. Fair information practices must be built into the systems architecture. The methodology in Step #5 translates a company's privacy policy into technical practices. It does this by developing systems architecture rules and designing controls around the collection of personal information, linkability, access, use and accountability, as well as delineating business processes that use personal data. It is also important to ensure that the methodology rules are designed in consideration of the type of data being used (i.e., the level of sensitivity).

One useful methodology for building privacy into systems architecture is Privacy Rights Management (PRM). In a paper entitled, *Privacy Rights Management for Digital Rights Management*, Steve Kenny and Larry Korba define PRM as "distributed management of personal information in accordance with EU data protection legislation."[36] In particular, they examine the architectural potential of DRM to manage the requirements of the EU *Data Protection Directive*. However, recognizing that it is difficult to integrate legal requirements into the development of new systems, they also put forward some simplified privacy principles that companies can use as a starting point for a detailed analysis of the privacy aspects of systems architecture.

According to Kenny and Korba, content distribution companies must balance the need to protect digital content (i.e., fraud prevention) against potential liability that may arise if personal information has been misused. They argue that a PRM methodology can provide copy prevention for a company and protect the privacy rights of its customers through token schemes, for example.

Step #6: Introduce at the source level, the rules and controls developed in Step #5

This step can be combined with Step #5 if the developers of the architecture rules are also responsible for implementation. When deploying these rules, there are numerous implementation challenges, including ensuring that associated costs remain under control; estimating the size of data storage containers; ensuring that rights management is still feasible while ensuring that personal data is not compromised; finding data distribution mechanisms that maintain data quality across all processors; operating within different jurisdictions; and carrying out successful logging and auditing of data processes.[37] Despite such challenges, the above tools and models provide a reasonable idea of how to build privacy into DRM.

Step #7: Deploy and audit, through a model of continuous improvement — review expectations and requirements

The final step is unlike the others because it is one that requires repetition throughout the operation of the DRM service. One of the most important rules in gauging whether DRM technology is sufficiently privacy protective is to remember that "overall, privacy is [only] as strong as the privacy offered by the weakest link."[38] Auditing ensures that the host organization will be in a position to identify any weak links within the DRM system.

It is up to the DRM host organization, through the privacy environment it established in Step #1, to conduct an end-to-end privacy audit of the DRM process. The host organization may select an outside auditor such as Watchfire,[39] which would dig through all the organizational and electronic processes to determine system weaknesses. A Harris Interactive survey found that 84% of consumers believe that independent verification of privacy policies should be a requirement for companies.[40]

Privacy Protection Tips for Consumers

It is important to remember that the Internet remains a highly unregulated environment. As a precautionary step, consumers need to understand that they may be giving up their privacy in exchange for the use of free or inexpensive digital content, based on a DRM model. Consumers are strongly encouraged to read privacy policies, be highly selective when offering their personal information to Web sites, and only deal with reputable organizations that clearly state that personal information:

- will not be collected without consent;
- will not be used for secondary purposes;
- will be held in secure databases; and
- will not be retained for unnecessarily long periods of time.

Privacyactivism, a non-profit organization, has recently released version 1.0 of a unique consumer video game called *Carabella*, which "highlights the ways that consumers' privacy and fair use rights are being whittled away by digital rights management technologies, online spyware and data profiling services."[41] The game attempts to raise awareness of personal tracking, how to surf anonymously, and raises privacy and fair use issues with peer-to-peer networks and online subscription services. Readers of this paper are encouraged to access this creative video game.

Conclusion

The expansion of DRM technologies has significant implications for the privacy, fair use and free expression rights of consumers. Although many companies that use DRM technologies appear to be gambling that consumers will eventually accept some infringement of their rights in exchange for DRM-protected digital music or movies, there is no guarantee that this will happen. Instead, consumers may reach a breaking point and refuse to purchase such products if they feel that their rights are being increasingly violated.

In this paper, we have focused on the privacy issues associated with DRM and argued that companies that use such technologies should consider simply not collecting personal information from consumers or seek their informed consent before collecting, using or disclosing any personal information. In addition, we have put forward seven steps for embedding privacy into DRM technologies, and proposed some simple privacy protection tips for consumers. Addressing privacy problems alone will not alleviate the host of problems connected to DRM. However, thinking about privacy issues may help the industry to assess whether its overall approach to protecting digital content is viable in the long term, or whether it should adopt a more balanced approach that also takes into account the rights of consumers.

Appendix A — *CSA Model Code for the Protection of Personal Information*

Principle 1 — Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

Principle 2 — Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Principle 3 — Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Principle 4 — Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Principle 5 — Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

Principle 6 — Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purpose for which it is to be used.

Principle 7 — Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Principle 8 — Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Principle 9 — Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information, and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Principle 10 — Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Endnotes

1. See paragraph 1 of the full complaint, which was filed in the Superior Court of the State of California (County of Marin) and is available at www.techfirm.com/mccomp.pdf.

2. Ibid.

3. Ibid., paragraph 37.

4. The settlement agreement is located at www.techfirm.com/sunnk.pdf.

5. "The Internet Under Siege" Foreign Policy – The Magazine of Global Politics, Economic and Ideas (November/December 2001) at www.foreignpolicy.com/issue_novdec_2001/lessig.html.

6. See EPIC's Web page on Digital Rights Management and Privacy at www.epic.org/privacy/drm/. See also EFF's article on Fair Use and Digital Rights Management at www.eff.org/IP/DRM/fair_use_and_drm.html.

7. Written testimony of Will Poole, Corporate Vice President, Microsoft Corporation, at a hearing before the Subcommittee on Courts, the Internet, and Intellectual Property of the Committee on the Judiciary of the House of Representatives (June 5, 2002), at www.house.gov/judiciary/poole060502.htm.

8. Supra note 6.

9. www.loc.gov/copyright/legislation/hr2281.pdf.

10. Supra note 7.

11. www.louisville.edu/library/law/brandeis/privacy.html.

12. Steve Kenny & Larry Korba, "Privacy Rights Management for Digital Rights Management" (2002). An abstract can be found at www.cbpweb.nl/documenten/art_Kenny_Privacy_rights_management_2002.htm.

13. Joan Feigenbaum, Michael J. Freedman, Tomas Sander and Adam Shostack, *Privacy Engineering for Digital Rights Management Systems* at www.homeport.org/~adam/privacyeng-wspdrm01.pdf.

14. Ibid., at 3.

15. Ibid.

16. Ibid., at 4.

17. Chris Hoofnagle, Fred von Lohmann and Jason Young, EPIC/EFF letter to the Subcommittee on Courts, the Internet, and Intellectual Property of the Committee on the Judiciary of the House of Representatives, (June 5, 2002), at www.epic.org/privacy/drm/hjdrmltr6.5.02.html.

18. Some examples include Dr.Koop.com, Boo.com, and Toysmart.

19. Chris Hoofnagle, "Panel on Consumer Privacy in the E-Commerce Marketplace" 3 Internet Law and Business 812 (August 2002) at www.epic.org/epic/staff/hoofnagle/ilbpaper.html.

20. "What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication" (2000) 52 Stanford Law Review at papers.ssrn.com/sol3/papers.cfm?abstract_id=214468.

21. "Trusted Systems," *Scientific American*, March 1997.

22. www.ipc.on.ca/english/resources/7steps.pdf.

23. News Release, "First Major Post-9/11 Privacy Survey Finds Consumers Demanding Companies Do More To Protect Privacy; Public Wants Company Privacy Policies To Be Independently Verified" (February 20, 2002) at www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=429.

24. News Release, "Forrester Technographics Finds Online Consumers Fearful of Privacy Violations" (October 27, 1999) at www.forrester.com/ER/Press/Release/0,1769,177,FF.html.

25. Poorvi Vora, Dave Reynolds, Ian Dickinson, John Erickson & Dave Banks, "Privacy and Digital Rights Management" A position paper for the W3C workshop on Digital Rights Management (January 2001) at www.w3.org/2000/12/drm-ws/pp/hp-poorvi2.html.

26. http://europa.eu.int/comm/internal_market/en/dataprot/law/dir1995-46_part1_en.pdf.

27. Stefano Rodota, "Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites" (May 30, 2002) at 12. The paper can be found at http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp56_en.pdf.

28. www.privcom.gc.ca/legislation/02_06_01_e.asp.

29. www.oecd.org/EN/document/0,,EN-document-43-1-no-24-10255-43,00.html.

30. www.csa.ca/standards/privacy/code/default.asp?language=English.

31. For example, see the Direct Marketing Association's Privacy Policy Generator at www.thedma.org/library/privacy/creating.shtml or the OECD's Privacy Statement Generator at http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm.

32. www.ipc.on.ca/english/resources/resources.htm.
33. www.gov.on.ca:80/MBS/english/fip/pia/pia.pdf.
34. www.mser.gov.bc.ca/foi_pop/manual/forms/pia.doc.
35. www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/siglist_e.html.
36. Supra note 12.
37. Ibid.
38. Supra note 13.
39. www.watchfire.com/.
40. Supra note 23.
41. www.privacyactivism.org/.

Information and Privacy Commissioner/Ontario

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: www.ipc.on.ca